Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ ПРЕДОТВРАЩЕНИЯ ИНЦИДЕНТОВ И СНИЖЕНИЯ РИСКОВ (FUNDAMENTALS OF INCIDENT PREVENTION AND RISK MITIGATION)

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
3	3	108	16	16	0		40	0	Э
Итого	3	108	16	16	0	0	40	0	

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Основы предотвращения инцидентов и снижения рисков» содержит описание целей освоения дисциплины, ее место в структуре ООП, ВПО, формируемые в результате освоения дисциплины компетенции студента, структуру и содержание дисциплины, используемые во время освоения дисциплины об-разовательные технологии, оценочные средства для контроля успеваемости, учебно-методическое, информационное и материально-техническое обеспечение дисциплины/

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью преподавания дисциплины является: изучение методов и средств управле-ния инцидентами информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления инцидентами ИБ (СУИИБ) определенного объек-та.

Задачами дисциплины являются:

привитие обучаемым основ культуры обеспечения ИБ;

формирование у обучаемых понимания роли процессов управления инцидентами ИБ в обеспечении ИБ организаций, объектов и систем;

ознакомление обучаемых с основными методами управления инцидентами ИБ;

обучение различным методам реализации процессов управления инцидентами ИБ, направленных на эффективное управление ИБ конкретной организации.

Вместе с другими дисциплинами общенаучного и профессионального циклов дис-циплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

строгость в суждениях,

творческое мышление,

организованность и работоспособность,

дисциплинированность,

самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Основы предотвращения инцидентов и снижения рисков» является неотъемлемой составной частью профессиональной подготовки магистров по направле-нию подготовки 10.04.01 «Информационная безопасность» и относится к числу дисциплин профессионального цикла. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыки, сформированные в процессе:

изучения программы общеобразовательной школы;

освоения программы подготовки бакалавров или программ подготовки специа-листов по родственным направлениям высшего профессионального образования;

изучения дисциплин: «Экономика и управление», «Защищенные информаци-онные системы», «Технологии обеспечения информационной безопасности объектов».

Знания, полученные при изучении дисциплины «Основы предотвращения инци-дентов и снижения рисков» являются базовыми для профессиональных дисциплин, вхо-дящих в базовую (курсы «Управление обеспечением непрерывности бизнеса», «Основы обеспечения

непрерывности и информационной безопасности бизнеса») и вариативную части профессионального цикла учебного плана подготовки магистров по направлению 10.04.01 «Информационная безопасность».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-4 [1] – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	З-УК-4 [1] – Знать: правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия У-УК-4 [1] – Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия В-УК-4 [1] – Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий
УК-6 [1] – Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	З-УК-6 [1] – Знать: методики самооценки, самоконтроля и саморазвития с использованием подходов здоровьесбережения У-УК-6 [1] – Уметь: решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности В-УК-6 [1] – Владеть: технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровьесберегающих подходов и методик

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный**	**Код и наименование индикатора достижения профессиональной компетенции**

		стандарт-ПС, анализ опыта)	
научно-исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть:

			организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Стандартизация в области предотвращения инцидентов и снижения рисков ИБ. Базовые вопросы предотвращения инцидентов и снижения рисков ИБ.	1-8	8/8/0		25	КИ-8	З-ПК-3, У-ПК-3, В-ПК-3, З-УК-4, У-УК-4, В-УК-4, З-УК-6, У-УК-6, В-УК-6
2	Документация системы предотвращения инцидентов и снижения рисков ИБ. Кадровые и технические вопросы при предотвращении инцидентов и снижении рисков ИБ.	9-16	8/8/0		25	КИ-16	З-ПК-3, У-ПК-3, В-ПК-3, З-УК-4, У-УК-4, В-УК-4, З-УК-6, У-УК-6, В-УК-6
	Итого за 3 Семестр		16/16/0		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ПК-3, У-ПК-3, В-ПК-3, З-УК-4, У-УК-4, В-УК-4, З-УК-6, У-УК-6, В-УК-6

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	3 Семестр	16	16	0
1-8	**Стандартизация в области предотвращения инцидентов и снижения рисков ИБ. Базовые вопросы предотвращения инцидентов и снижения рисков ИБ.**	8	8	0
1	**Тема № 1. Введение** Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
2	**Тема № 2. Нормативная база в области предотвращения инцидентов и снижения рисков ИБ** Существующие стандарты и методологии в области предотвращения инцидентов и снижения рисков ИБ: их отличия, сильные и слабые стороны. История развития. ISO/IEC 27035:2011 – предотвращение инцидентов ИБ. ISO/IEC 27037 – руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
3	**Тема № 3. Событие и инцидент ИБ.** Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи обеспечения ИБ. Понятие системы управления. Цели и задачи предотвращения инцидентов и снижения рисков ИБ.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
4	**Тема № 4. Системы предотвращения инцидентов и снижения рисков ИБ (СУИИБ)** Системы предотвращения инцидентов и снижения рисков ИБ (СУИИБ)	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
5	**Тема № 5. Процесс предотвращения инцидентов и снижения рисков ИБ** Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Основные процессы. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИИБ). Важность процесса управления инцидентами ИБ с точки	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0

	зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Связи с другими процессами СУИБ. Обязательные этапы процесса. Планирование и подготовка процесса. Внедрение процесса. Использование СУИИБ. Анализ процесса. Улучшение процесса.			
6	**Тема № 6. Обнаружение и обработка событий и инцидентов ИБ** Обнаружение событий ИБ и инцидентов ИБ и оповещение о них. Обработка событий ИБ и инцидентов ИБ. Первая оценка и предварительное решение по событию ИБ. Вторая оценка и подтверждение инцидента ИБ.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
7 - 8	**Тема № 7. Реагирование на инциденты ИБ** Немедленное реагирование на инцидент ИБ. Контролируемость инцидента ИБ. Последующее реагирование на инцидент ИБ. Антикризисные действия. Правовая экспертиза инцидентов ИБ. Передача информации. Расширение области принятия решений. Регистрация деятельности и контроль за внесением изменений. Техническая поддержка реагирования на инциденты ИБ.	Всего аудиторных часов		
		0	4	0
		Онлайн		
		0	0	0
9-16	**Документация системы предотвращения инцидентов и снижения рисков ИБ. Кадровые и технические вопросы при предотвращении инцидентов и снижении рисков ИБ.**	8	8	0
9 - 10	**Тема № 8. Политика предотвращения инцидентов и снижения рисков ИБ** Основные цели. Структура. Содержание.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
11 - 12	**Тема № 9. Программа предотвращения инцидентов и снижения рисков ИБ** Другие документы: формы регистрации инцидентов, регламенты сбора свидетельств инцидентов ИБ и т.п.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
13 - 14	**Тема № 10. Группа реагирования на инциденты ИБ.** **Тема № 11. Обеспечение осведомленности и обучение в области предотвращения инцидентов и снижения рисков ИБ** Цели, задачи. Состав группы. Понятие роли. Использование ролевого принципа в рамках СУИИБ. Преимущества использования ролевого принципа. Ролевая структура СУИИБ (основные и дополнительные роли).	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
15 - 16	**Тема № 12. Сохранение доказательств инцидента ИБ.** **Тема № 13. Средства управления событиями ИБ** Сохранение доказательств инцидента ИБ. Средства управления событиями ИБ.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс

ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	3 Семестр
5	**Тема № 5. Процесс предотвращения инцидентов и снижения рисков ИБ** Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Основные процессы. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИИБ). Важность процесса управления инцидентами ИБ с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Связи с другими процессами СУИБ. Обязательные этапы процесса. Планирование и подготовка процесса. Внедрение процесса. Использование СУИИБ. Анализ процесса. Улучшение процесса.
6	**Тема № 6. Обнаружение и обработка событий и инцидентов ИБ** Обнаружение событий ИБ и инцидентов ИБ и оповещение о них. Обработка событий ИБ и инцидентов ИБ. Первая оценка и предварительное решение по событию ИБ. Вторая оценка и подтверждение инцидента ИБ.
7 - 8	**Тема № 7. Реагирование на инциденты ИБ** Немедленное реагирование на инцидент ИБ. Контролируемость инцидента ИБ. Последующее реагирование на инцидент ИБ. Антикризисные действия. Правовая экспертиза инцидентов ИБ. Передача информации. Расширение области принятия решений. Регистрация деятельности и контроль за внесением изменений. Техническая поддержка реагирования на инциденты ИБ.
9 - 10	**Тема № 8. Политика предотвращения инцидентов и снижения рисков ИБ** Основные цели. Структура. Содержание.
11 - 12	**Тема № 9. Программа предотвращения инцидентов и снижения рисков ИБ** Другие документы: формы регистрации инцидентов, регламенты сбора свидетельств инцидентов ИБ и т.п.
13 - 14	**Тема № 10. Группа реагирования на инциденты ИБ. Тема № 11. Обеспечение осведомленности и обучение в области предотвращения инцидентов и снижения рисков ИБ.** Цели, задачи. Состав группы. Понятие роли. Использование ролевого принципа в рамках СУИИБ. Преимущества использования ролевого принципа. Ролевая структура СУИИБ (основные и дополнительные роли).
15 - 16	**Тема № 12. Сохранение доказательств инцидента ИБ. Тема № 13. Средства управления событиями ИБ.** Сохранение доказательств инцидента ИБ. Средства управления событиями ИБ.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: доклады и презентации с их обсуждением, ролевые игры с дискуссиями и разбором конкретных ситуаций в сочетании с внеаудиторной работой.

В дисциплине также используются интерактивные формы обучения на основе самостоятельного освоения электронного учебника «Управление инцидентами информационной безопасности» и тестирования промежуточных знаний студентов.

В процессе преподавания дисциплины в каждом разделе выделяются наиболее важные темы и внимание обучаемых особо акцентируется на них.

В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области управления инцидентами ИБ, а также российских и зарубежных компаний – разработчиками систем управления инцидентами ИБ.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-3	З-ПК-3	Э, КИ-8, КИ-16
	У-ПК-3	Э, КИ-8, КИ-16
	В-ПК-3	Э, КИ-8, КИ-16
УК-4	З-УК-4	Э, КИ-8, КИ-16
	У-УК-4	Э, КИ-8, КИ-16
	В-УК-4	Э, КИ-8, КИ-16
УК-6	З-УК-6	Э, КИ-8, КИ-16
	У-УК-6	Э, КИ-8, КИ-16
	В-УК-6	Э, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически

			стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Структура и содержание курса

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе выполнения лабораторных работ и самостоятельных занятий.

Содержание дисциплины распределяется между лекционной и практической частями на основе принципа масштабируемости: практические занятия, как правило, не дублируют лекции и носят ярко выраженный творческий характер. В лекционном курсе главное место отводится общетеоретическим проблемам. Практические занятия рекомендуется использовать для выработки у студентов практических навыков защиты в открытых системах.

При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в основной литературе;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

За основу логического прохождения курса приняты следующие положения.

Общая часть курса посвящена выявлению основных особенностей сущностей «событие ИБ» и «инцидент ИБ», изучению международных и российских стандартов по управлению инцидентами ИБ, рассмотрению систем управления инцидентами ИБ. После этого подробно изучается процесс управления инцидентами ИБ с точки зрения процессного подхода. В завершении курса анализируется документальное обеспечение процесса управления инцидентами ИБ, кадровые и технические вопросы.

Теоретические положения курса подкрепляются иллюстрациями и выработкой практических навыков при выполнении студентами практических работ по основным темам курса.

Примерным учебным планом на изучение дисциплины отводятся один семестр.

Итоговая аттестация по дисциплине.

Осуществляется в форме экзамен. После изучения курса студент должен сдать экзамен.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Средства обеспечения освоения учебного курса

При изучении дисциплины рекомендуется использовать следующие средства обучения:

программу учебного курса;

рекомендуемую основную и дополнительную литературу;

методические указания, пособия и учебники (в бумажном виде);

задания для самостоятельной работы для закрепления теоретического материала;

описания лабораторных работ и контрольные вопросы к ним;

методическое обеспечение текущего и итогового контроля знаний.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и

средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы и самостоятельной работе.

Основные формы изучения дисциплины

Курс читается на третьем семестре.

Курс рассчитан на 108 часов, из которых 32 часа лекционных занятий, 16 часов практических занятий – семинаров (ПР), 16 часов практических занятий и 40 часа самостоятельной работы (СР) студента, в том числе занятия в интерактивной форме – 16 часов.

Для самостоятельной работы студентов с использованием интерактивных форм обучения предлагается электронный учебник «Управление инцидентами информационной безопасности».

Принципы отбора содержания и организации учебного материала дисциплины

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе выполнения лабораторных работ и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов.

Содержание дисциплины распределяется между лекционной и практической частями на основе принципа масштабируемости: практические занятия, как правило, не дублируют лекции и носят ярко выраженный творческий характер. В лекционном курсе главное место отводится общетеоретическим проблемам. Практические занятия рекомендуется использовать для выработки у студентов практических навыков защиты в открытых системах.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в основной литературе;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области управления инцидентами ИБ, а также российских и зарубежных компаний – разработчиками систем управления инцидентами ИБ.

Обоснование логики прохождения учебного курса

За основу логического прохождения курса приняты следующие положения.

Общая часть курса посвящена выявлению основных особенностей сущностей «событие ИБ» и «инцидент ИБ», изучению международных и российских стандартов по управлению инцидентами ИБ, рассмотрению систем управления инцидентами ИБ. После этого подробно изучается процесс управления инцидентами ИБ с точки зрения процессного подхода. В завершении курса анализируется документальное обеспечение процесса управления инцидентами ИБ, кадровые и технические вопросы.

Теоретические положения курса подкрепляются иллюстрациями и выработкой практических навыков при выполнении студентами практических работ.

Автор(ы):

Горбатов Виктор Сергеевич, к.т.н., доцент

Рецензент(ы):

Дураковский А.П.